Certification Report

EP-COS V3.0 Plain, EPCOSV30e

Sponsor:	***NXP Semiconductors Germany GmbH*** **Troplowitzstrasse 20,** **D-22529 Hamburg,** **Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-127667-CR3**
Report version:	**1**
Project number:	**127667_3**
Author(s):	**Denise Cater**
Date:	**14 February 2022**
Number of pages:	**11**
Number of appendices:	**0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the EP-COS V3.0 Plain, EPCOSV30e. The developer of the EP-COS V3.0 Plain, EPCOSV30e is eSmart Systems Ltd located in Noida, India, and NXP Semiconductors Germany GmbH act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to Part 1 of 'ICAO Doc 9303'.

The TOE was evaluated initially by Brightsight B.V. located in Delft, The Netherlands and was certified on 14 February 2017. A (minor) re-evaluation was completed by Brightsight B.V. on 13 March 2017 This re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 10 February 2022 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The second issue of the Certification Report was as a result of a minor change to the evidence. The assessment of the developer's impact analysis report indicated that the original evaluation results, which had only been completed a month earlier, could be re-used. The associated Security Target (and public version) only needed editorially updating to include changes of the provided guidance documentation.

This third issue of the Certification Report is a result of a "recertification with major changes".

The major changes reflect the renewal of the underlying platform certificates and a patch (limited scope) to the BAC eMRTD application. The changes resulted in an update of the [ST], [ST-Lite] and the TOE guidance to reflect the change of TOE version.

The security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the EP-COS V3.0 Plain, EPCOSV30e, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the EP-COS V3.0 Plain, EPCOSV30e are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and ATE_DPT.2 (Testing: security enforcing modules).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the EP-COS V3.0 Plain, EPCOSV30e, as sponsored by NXP Semiconductors Germany GmbH located in Hamburg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	P60D081PVB (P6021yVB configuration)	VB
Software	Crypto Library V3.1.2 on P60D081PVB	V3.1.2
	IC Embedded Software (operating system)	EPCOSV30e
	MRTD application BAC	Version 1.0

To ensure secure usage a set of guidance documents is provided, together with the EP-COS V3.0 Plain, EPCOSV30e. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.3.

2.2 Security Policy

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD’s chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to Part 1 ‘ICAO Doc 9303’.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.1 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

The environment in which the TOE is personalised must perform proper and safe personalisation according to the guidance and referred ICAO guidelines.

The environment in which the TOE is used must ensure that the inspection system protects the confidentiality and integrity of the data send and read from the TOE.

2.4 Architectural Information

The Target of Evaluation (TOE) EP-COS V3.0 Plain is the contactless integrated circuit chip of machine readable travel documents (MRTD’s chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to the ICAO documentation.

The TOE is comprised of the following subsystems:

- the circuitry of the MRTD’s chip P60D081PVB (P6021yVB configuration) with Crypto Library V3.1.2 on P60D081PVB

- the IC Embedded Software (operating system)
- the MRTD application BAC.

Using this, the TOE provides an ISO 7816-4 file structure according to the ICAO 9303 specifications.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Personalization Guidance (AGD_PRE) EP-COS V3.0 Plain	Version 0.99
Operational User Guidance (AGD_OPE) EP-COS V3.0 Plain	Version 0.98

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

For both the baseline and this re-evaluation, the developer has performed extensive testing on functional specification, subsystem and SFR-enforcing module level. The testing was largely automated using proprietary test suites, mostly on the actual TOE and in exception cases on an emulator.

The hardware and crypto-library test results are extendable to composite evaluations, as this underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer has provided samples. The evaluators witnessed the execution of the test suite by the developer during the baseline evaluation, and performed a small number of test cases designed by the evaluator, addressing edge cases. The test witnessing was performed on an earlier version of the TOE, EPCOSV30d. The difference between EPCOSV30d and EPCOSV30e is limited to a single function, does not impact the behaviour of the claimed security functionality, and hence does not affect any of the witnessed test results.

2.6.2 Independent penetration testing

The penetration tests are devised after performing the Evaluator Vulnerability Analysis. This analysis has followed the following steps. The reference for attack techniques against which smart card-based devices such as the TOE must be protected against is the document "Attack methods for smart cards" [JIL-AM]. Additional guidance for testing was provided by the certification body in the form of a number of questions regarding the TOE. The vulnerability of the TOE for these attacks has been analysed in a white box investigation conforming to AVA_VAN.3.

- 1. Inventory of required resistance
  - This step uses the JIL attack list [JIL-AM] as a reference for completeness and studies the ST claims to decide which attacks in the JIL attack list apply for the TOE.
- 2. Validation of security functionalities
  - This step identifies the implemented security functionalities and performs tests to verify the implementation and to validate proper functioning. (ATE)
- 3. Vulnerability analysis
  - This step first gives an overview against which attacks the implemented security functionalities are meant to provide protection. Secondly in this step the design of the implemented security functionalities is studied. This also includes the security functionalities implemented in the hardware (cf. [HW-UGM], [HW-ETRfC]). Thirdly, analysis is performed to determine whether the design contains vulnerabilities against the respective attacks of Step 1. (AVA)

- 4. Analysis of input from other evaluation activities
  - This step first analyses the input from other CC-evaluation classes expressed as possible vulnerabilities. Secondly, the evaluators performed analysis of the TOE in its intended environment to check whether the developer vulnerability analysis provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance. (AVA)
- 5. Design assurance evaluation
  - This step analyses the results from an attack perspective as defined in Step 1. Based on this design analysis the evaluators determine whether the design provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance. (AVA)
- 6. Penetration testing
  - This step performs the penetration tests identified in Step 4 and Step 5. (AVA)
- 7. Conclusions on resistance
  - The evaluators analyse the results of the penetration tests performed in Step 6. Based on this analysis the evaluators draw conclusions on the resistance of the TOE attackers possessing Enhanced-Basic attack potential.

No potential vulnerabilities within the attack potential were found that were not already addressed by the underlying platform.

For extra assurance, several of the potential vulnerabilities beyond the attack potential were tested. In the baseline evaluation the total test effort was 26 days, and consisted of one EMFI and three laser tests. The total test effort expended by the evaluators in this re-evaluation was 4.5 weeks. During that test campaign, 89% of the total time was spent on Perturbation attacks, and 11% on side-channel testing,.

2.6.3 Test configuration

The TOE was tested in the following configurations:

- EP-COS V3.0 Plain, EPCOSV30d

The test results obtained on version EPCOSV30d are fully applicable to EPCOSV30e, as the only difference comprises a security enhancement.

During the baseline evaluation Testing was performed on the TOE as inlays, SO28, CLCC and DIL packages. The SO28 was used for ATE developer tests; the inlays were used for ATE independent and AVA tests; the DIL and CLCC packages were used for AVA tests only. In all cases the samples were been delivered in locked state. The evaluators ran a script to bring the samples from the locked state to unlocked state and further on to the operational state. The ATE tests covered all life-cycle states of the TOE. The AVA tests targeted the operational state.

During this re-evaluation, the developer testing was performed using an emulator and on the SO28 package of the TOE. The evaluator testing was performed on the CLCC package of the TOE.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

Sites involved in the development and production of the hardware platform were reused by composition.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number EP-COS V3.0 Plain, EPCOSV30e.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for a development site *[STAR]* [2].

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the EP-COS V3.0 Plain, EPCOSV30e, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2 and ATE_DPT.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[PP-0055]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance (including the ICAO guidelines).

There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

3 Security Target

The Security Target EP-COS V3.0 Plain, Rev. 2.5, 03 February 2022 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

BAC	Basic Access Control
ICAO	International Civil Aviation Organisation
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[CCRA-AC]	Assurance Continuity: CCRA Requirements, CCRA Supporting Document, version 2.1, June 2012
[CL-CERT]	Certification Report Crypto Library V3.1x on P6021yVB, NSCIB-CC-66030-CR5, 7 July 2021
[CL-ETRfC]	ETR for Composite Evaluation Crypto Library V3.1.x on P6021y VB EAL6+, 18-RPT-197, Version 9.0, 6 July 2021
[CL-ST]	Crypto Library V3.1.x on P6021y VB Security Target, Rev. 1.9, 22 March 2018
[ETR]	Evaluation Technical Report “EP-COS V3.0 Plain, EPCOSV30e” – EAL4+, 22-RPT-082, Version 3.0, 10 February 2022
[HW-CERT]	Certification Report NXP Secure Smart Card Controller P6021yVB including IC dedicated software, BSI-DSZ-CC-1072-V4-2021-MA-01, 17 December 2021
[HW-ETRfC]	EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), P6021y VB, BSI-DSZ-CC-1072-V4, 16 June 2021
[HW-ST]	NXP Secure Smart Card Controller P6021y VB Security Target Lite, 1.11, 23 August 2019
[HW-UGM]	NXP Secure Smart Card Controller P6021y VB, Rev.1.2, 21 November 2018
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP_0055]	Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (MRTD-PP), Version 1.10, 25 March 2009, registered under the reference BSI-CC-PP-0055-2009
[ST]	Security Target EP-COS V3.0 Plain, Rev. 2.5, 03 February 2022
[ST-lite]	Security Target Lite EP-COS V3.0 Plain, Rev 2.5, 07 February 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR]	Site Technical Audit Report e-Smart systems, 21-RPT-1308, Version 2.0, 09 February 2022

(This is the end of this report.)